



User Manual

Wireless N 150 Home Router

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Manual Revisions

Revision	Date	Description
1.0	June 24, 2013	Initial Release

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2013 by D-Link Systems, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Systems, Inc.

Table of Contents

Preface	i	Manual Wireless Network Setup	21
Manual Revisions	i	Network Settings	25
Trademarks	i	DHCP Server Settings	26
Product Overview	1	DHCP Reservation	27
Package Contents	1	Advanced	28
System Requirements	2	Virtual Server	28
Features	3	Port Forwarding	30
Hardware Overview	4	Network Filters	31
Connections	4	Website Filter	32
LEDs	5	Firewall Settings	33
Installation	6	Advanced Wireless Settings	34
Before you Begin	6	Wi-Fi Protected Setup	35
Wireless Installation Considerations	7	Advanced Network Settings	36
Connect to Cable/DSL/Satellite Modem	8	Tools	37
Configuration	9	Administrator Settings	37
Easy Setup Wizard	10	Time and Date	38
Internet Connection Setup Wizard	11	System	39
Wireless Security Wizard	12	Firmware	40
Manual Configuration	13	Dynamic DNS	41
Internet	13	Status	42
Static IP Address	14	Device Information	42
Dynamic IP Address (DHCP)	15	Logs	43
PPPoE	16	Internet Sessions	44
Wireless Settings	18	Wireless	45
Add Wireless Device with WPS	19	Support	46

Wireless Security.....	47	Troubleshooting	60
What is WEP?	47	Wireless Basics	64
What is WPA?	47	Tips.....	65
Configuring WEP.....	48	Wireless Modes.....	66
Configuring WPA/WPA2-Personal (PSK)	49	Networking Basics	67
Configuring WPA/WPA2-Enterprise (PSK)	50	Check your IP address.....	67
Connect to a Wireless Network.....	52	Check Your MAC Address.....	68
Windows® 8.....	52	Statically Assign an IP address	69
WPA/WPA2	52	Technical Specifications	70
Using Windows® 7	54	Safety Statements	71
Using Windows® XP	57		
Configure WPA-PSK.....	58		

Package Contents



D-Link DIR-610N Wireless N 150 Home Router



Power Adapter



Ethernet Cable



Quick Installation Guide

Note: Using a power supply with a different voltage rating than the one included with the D-Link DIR-610N will cause damage and void the warranty for this product. Always attach the power cord plug to the power supply **before** inserting the power cord and connected power supply to the wall outlet.

System Requirements

Network Requirements	<ul style="list-style-type: none">• An Ethernet-based Cable or DSL modem• IEEE 802.11n/g/b wireless clients
Web-based Configuration Utility Requirements	<p>Computer with the following:</p> <ul style="list-style-type: none">• Windows®, Macintosh, or Linux-based operating system• An installed Ethernet adapter <p>Browser Requirements:</p> <ul style="list-style-type: none">• Internet Explorer 8.0 or later• Firefox 12.0 or later• Safari 4.0 or later (with Java 1.3.1 or higher)• Chrome 20.0 or later

Features

- **Faster Wireless Networking** - The D-Link DIR-610N provides up to 150 Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.
- **Compatible with 802.11g Devices** - The D-Link DIR-610N is still fully compatible with the IEEE 802.11g standard, so it can connect with existing 802.11g and 802.11b wireless adapters.
- **Advanced Firewall Features** - The web-based user interface displays a number of advanced network management features including:
- **Content Filtering** - Easily applied content filtering based on URL, and/or domain name.
- **Easy Setup Wizard** - Through its easy-to-use web-based user interface, the D-Link DIR-610N lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

* Maximum wireless signal rate derived from IEEE Standard 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Hardware Overview

Connections



ID	Component	Description
1	LAN Ports	Connect up to 4 wired devices for fast Ethernet connections
2	Internet Port	Plug your broadband modem in to share your Internet connection
3	Reset Button	Return the router's settings to the factory defaults
4	Power Receptor	Plug in the supplied power adapter
5	WPS Button	Press this button to add wireless devices using WPS

Hardware Overview

LEDs



ID	Component	Status	Indication
1	Power LED	Solid	Indicates a proper connection to the power supply.
		Flashing	WPS connection is being established
2	Internet LED	Solid	Connection on the Internet port.
		Flashing	Data is being transferred through the Internet port

Installation

This section will walk you through the installation process. Placement of the router is very important. Do not place the router in an enclosed area such as a closet or cabinet, or in the attic or garage.

Before you Begin

- Please configure the router with the computer that was last directly connected to your modem.
- You can only use the Ethernet port on your modem. If you were using the USB connection before using the router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change the connection type from USB to Ethernet.
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoET, Broadjump, or EnterNet 300 from your computer or you will be unable to connect to the Internet.

Wireless Installation Considerations

The D-Link wireless router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45 degree angle appears to be almost 3 feet (1 meter) thick. At a 2 degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Connect to Cable/DSL/Satellite Modem

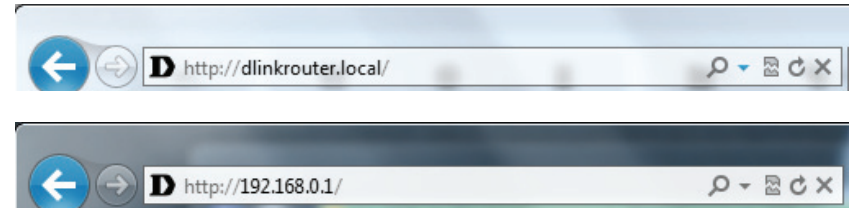
If you are connecting the router to a cable/DSL/satellite modem, please follow the steps below:

1. Place the router in an open and central location. Do not plug the power adapter into the router.
2. Turn the power off on your modem. If there is no on/off switch, then unplug the modem's power adapter. Shut down your computer.
3. Unplug the Ethernet cable (that connects your computer to your modem) from your computer and plug it into the Internet port on the router.
4. Plug an Ethernet cable into one of the four LAN ports on the router. Plug the other end into the Ethernet port on your computer.
5. Turn on or plug in your modem. Wait for the modem to boot (about 30 seconds).
6. Plug the power adapter to the router and connect to an outlet or power strip. Wait about 30 seconds for the router to boot.
7. Turn on your computer.
8. Verify the link lights on the router. The power light, Internet light, and the LAN light (the port that your computer is plugged into) should be lit. If not, ensure that your computer, modem, and router are powered on, and that the cables are correctly connected.
9. Skip to "Easy Setup Wizard" on page 10 to configure your router.

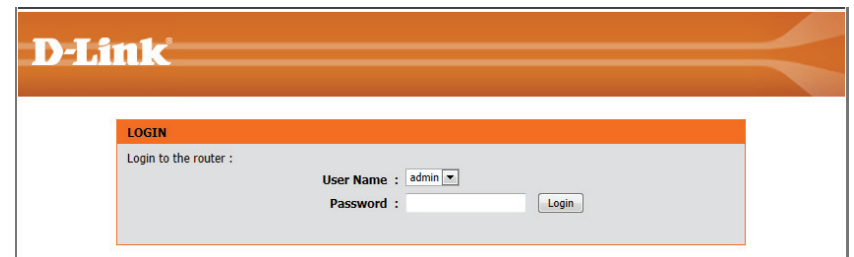
Configuration

This section will show you how to configure your D-Link wireless router using the web-based configuration utility.

To access the Easy Setup Wizard or configuration utility, open a web browser such as Internet Explorer and enter **http://dlinkrouter**. You can also enter the IP address of the router (**http://192.168.0.1**).



A login screen will appear. Select the administrator (admin) login name from the drop-down menu. By default, the password field should be left blank.



Easy Setup Wizard

When you log in to the router for the first time, the router will automatically attempt to detect your Internet connection type. Once the Internet type has been detected, you may be prompted to enter additional information such as a username and password (PPPoE). After your Internet connection has been set up, the following page will appear, showing a summary of the router's Internet, wireless, and admin settings.

Internet Settings: Displays the Internet connection type detected by the router, and the current status of your Internet connection. If the router was unable to detect your Internet settings, click the **Configure** button to commence the Internet connection setup wizard. Please refer to "Internet Connection Setup Wizard" on page 11 for further information.

Wireless Settings: Displays the current status of your router's wireless network including network name (SSID), password, and security type. You can make changes to these settings by clicking on the **Configure** button. Please refer to "Wireless Security Wizard" on page 12 for more information on using the setup wizard.

Admin Settings: Displays the current settings for the router's administrator account. This information will be used to log in to the web-based configuration utility. Check the **Set the Password of Device to Wireless Network Key** to make the administrator account password the same as the wireless network key set in the previous step.

Check the **Save my Network Settings** box to save the details of the current configuration as a text file on your computer. Once **Save** is clicked, you will receive a prompt to save the text file.

Click **Save** to save the current configuration.

EASY SETUP COMPLETE

The Easy Setup process has successfully completed. Click the "Save" button for your settings to take effect. We recommend you to check "Save my network settings" box to save your wireless network settings to your computer in case there are more PCs that need to connect to your router wirelessly.

After click the "Save" button, you need to provide your username and password to access the device when logging in next time.

Internet Settings

Internet Connection : Dynamic IP (DHCP)

Status : **Connected**

Wireless Settings

Wireless Network Name : dlink (SSID)

Status : **Unsecured**

Security : Disabled

[Configure](#)

Your current wireless security setting is not safe. We recommend that your security setting needs to be changed.

Admin Settings

User Name : admin

Status : **Unsecured**

Password : (blank)

Your current admin security setting is not safe. We recommend that you can synchronize your admin password with the wireless network key by clicking the checkbox below.

☐ : Set the password of device to wireless network key

☐ : Save my network settings

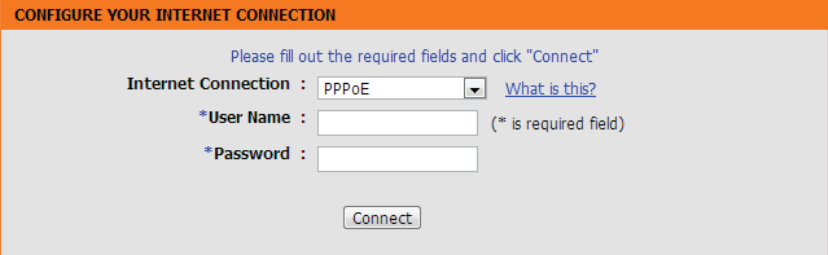
[Save](#)

Internet Connection Setup Wizard

Internet Connection: Select your Internet connection type from the drop-down menu.

User Name: If you selected PPPoE, enter your PPPoE user name.

Password: If you selected PPPoE, enter your PPPoE password.



The screenshot shows a web-based configuration window titled "CONFIGURE YOUR INTERNET CONNECTION" with an orange header. Below the header, a light gray box contains the following elements: a blue instruction line "Please fill out the required fields and click 'Connect'", a label "Internet Connection :" followed by a dropdown menu showing "PPPoE" and a "What is this?" link, a label "*User Name :" followed by a text input field and the note "(* is required field)", a label "*Password :" followed by a text input field, and a "Connect" button at the bottom right.

Wireless Security Wizard

Click **Configure** under Wireless Settings to begin the wireless security configuration wizard.



Wireless Settings

Wireless Network Name : dlink (SSID) Status : **Unsecured** [Configure](#)

Security : Disabled

Your current wireless security setting is not safe. We recommend that your security setting needs to be changed.

Click **Configure** under Wireless Settings to begin the wireless security configuration wizard.

Network Name (SSID): Enter the desired network name to identify your wireless network.

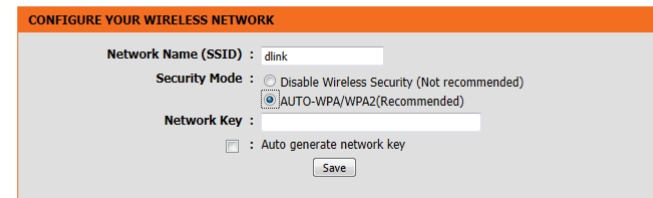
Security Mode: Select the security method to be used to secure the wireless network. It is strongly recommended that you select the **Auto-WPA/WPA2** method.

Network Key: Enter the desired network key (password) which will be used to access your wireless network.

Auto Generate Network Key: Check this box to have the router automatically generate a network key for you.

Click **Save** to save the current configuration.

Note: It is recommended that you make a record of this information for future reference.

CONFIGURE YOUR WIRELESS NETWORK

Network Name (SSID) : dlink

Security Mode : ☐ Disable Wireless Security (Not recommended) ☒ AUTO-WPA/WPA2(Recommended)

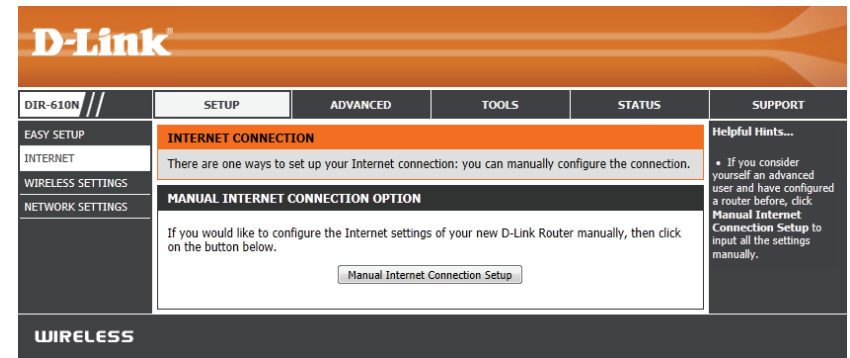
Network Key :

☐ : Auto generate network key [Save](#)

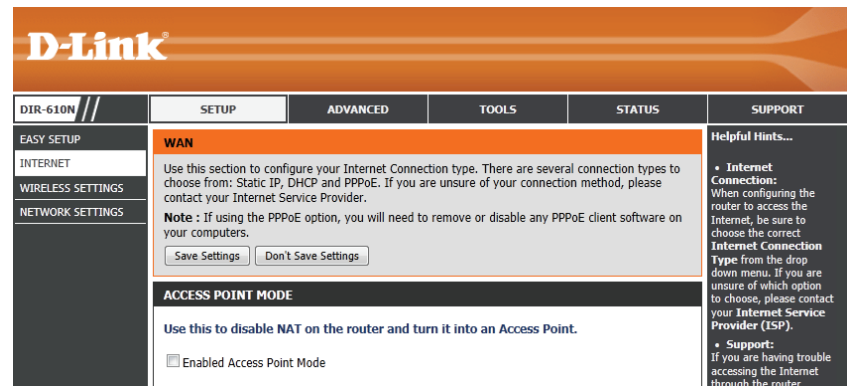
Manual Configuration

Internet

If you wish to configure your Internet connection manually, click on the **Manual Internet Connection Setup** button on the Setup > Internet page. You will be redirected to the configuration page that allows you to select the type of your Internet connection and enter the correct configuration parameters.



Enable Access Point Mode: Check the box to enable access point mode. If this mode is enabled, the router will not use NAT and will only function as an access point to your existing network.



Static IP Address

Choose **Static IP Address** if your ISP has provided you with a full set of IP address information. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP format, which is four octets each separated by a dot (x.x.x.x). The router will not accept an IP address if it is not in this format.

My Internet Connection is: Select **Static IP** from the drop-down menu.

IP Address: Enter the IP address assigned by your ISP.

Subnet Mask: Enter the subnet mask assigned by your ISP.

Default Gateway: Enter the gateway assigned by your ISP.

Primary DNS Server: Enter the primary DNS server address supplied by your ISP (Internet Service Provider.)

Secondary DNS Server: Enter the secondary DNS server address supplied by your ISP. This is optional, but may provide more stability should the primary DNS server fail.

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the router. It is not recommended that you change the default MAC address unless required to by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes that have been made.

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : Static IP

STATIC IP ADDRESS INTERNET CONNECTION TYPE :

Enter the static address information provided by your Internet Service Provider (ISP).

IP Address :

Subnet Mask : 0.0.0.0

Default Gateway :

Primary DNS Server :

Secondary DNS Server :

MTU : 1500

MAC Address :

Clone Your PC's MAC Address

Save Settings

Don't Save Settings

Dynamic IP Address (DHCP)

My Internet Connection is: Select **Dynamic IP (DHCP)** to obtain IP address information automatically from your ISP. Select this option if your ISP did not provide you with any IP numbers to use. This option is commonly used for cable modem services.

Host Name: The host name is optional but may be required by some ISPs.

Primary DNS Server: Enter the primary DNS server address provided to you by your ISP.

Secondary DNS Server: Enter the secondary DNS server address provided to you by your ISP. This is optional, but may provide more stability should the primary DNS server fail.

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

MAC Address: The default MAC address is set to the Internet port's physical interface MAC address on the router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes that have been made.

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is :

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name :

Primary DNS Server :

Secondary DNS Server :

MTU :

MAC Address :

PPPoE

Choose **PPPoE** (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Make sure you remove any PPPoE software from your computer. The software is no longer needed and will not work through a router.

My Internet Connection is: Select **PPPoE (Username/Password)** from the drop-down menu.

Address Mode: Select **Static IP** if your ISP assigned you an IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic IP**.

IP Address: Enter your IP address (Static PPPoE only).

User Name: Enter your PPPoE user name.

Password: Enter your PPPoE password and then retype the password in the **Verify Password** box.

Service Name: Enter the ISP service name (optional).

Reconnect Mode: Select either **Always-on**, **On-Demand**, or **Manual**.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. You can also enter 0 to have an infinite idle time. To disable this feature, set the reconnect mode to **Always on**.

DNS Mode: Select **Receive DNS from ISP** to automatically load DNS server information from your service provider. Select **Enter DNS Manually** to manually enter DNS server information (see below).

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : PPPoE (Username / Password) ▼

PPPOE INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : ☒ Dynamic IP ☐ Static IP

IP Address :

Username :

Password :

Verify Password :

Service Name : (optional)

Reconnect Mode : ☐ Always on ☒ On demand ☐ Manual

Maximum Idle Time : 5 (minutes, 0=infinite)

DNS Mode : ☒ Receive DNS from ISP ☐ Enter DNS Manually

Primary DNS Server :

Secondary DNS Server :

MTU : 1492

MAC Address :

Primary DNS Server: If you selected **Enter DNS Manually** above, enter the primary DNS server address supplied by your ISP (Internet Service Provider).

Secondary DNS Server: If you selected **Enter DNS Manually** above, enter the secondary DNS server address supplied by your ISP (Internet Service Provider). This is optional, but may provide more stability should the primary DNS server fail.

MTU: You may need to change the Maximum Transmission Unit for optimal performance with your specific ISP. The default MTU is 1492.

MAC Address: The default MAC address is set to the Internet port's physical interface MAC address on the broadband router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes that have been made.

Primary DNS Server :

Secondary DNS Server :

MTU :

MAC Address :

Clone Your PC's MAC Address

Save Settings

Don't Save Settings

Wireless Settings

From the **Wireless Settings** page, you can choose how you wish to set up your wireless network. To add a device using Wi-Fi Protected Setup (WPS), click on the **Add Wireless Device with WPS** button. If you want to manually configure the wireless settings on your router click **Manual Wireless Network Setup** and refer to "Manual Wireless Network Setup" on page 21.

D-Link

DIR-610N //

	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
EASY SETUP	<p>WIRELESS SETTINGS</p> <p>The following Web-based wizard are designed to assist you in your wireless network setup and wireless device connection.</p> <p>Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.</p> <p>ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD</p> <p>This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.</p> <p>Add Wireless Device with WPS</p> <p>MANUAL WIRELESS NETWORK SETUP</p> <p>If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.</p> <p>Manual Wireless Network Setup</p>				<p>Helpful Hints...</p> <ul style="list-style-type: none"> • If you already have a wireless network setup with Wi-Fi Protected Setup, click on Add Wireless Device with WPS to add new device to your wireless network. • If you consider yourself an advanced user and have configured a wireless router before, click Manual Wireless Network Setup to input all the settings manually.
INTERNET					
WIRELESS SETTINGS					
NETWORK SETTINGS					

Add Wireless Device with WPS

Wi-Fi Protected Setup (WPS) allows you to quickly and securely add compatible wireless devices to your wireless network. If your wireless device supports WPS, you can use this method to add it to your wireless network.

Auto: Select this option if the device that you want to add to your wireless network supports WPS.

Manual: Select this option if the device that you want to add to your wireless network does not support WPS.

Click **Next** to continue, or click **Cancel** to cancel the setup wizard.

STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK

Please select one of following configuration methods and click next to continue.

Auto ☒ Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

Manual ☐ Select this option will display the current wireless settings for you to configure the wireless device manually

Prev Next Cancel Connect

If you selected **Auto** in the previous step, there are two WPS methods which you can use to connect your wireless device.

PIN: Select this option if your device supports the PIN method of WPS. Enter the PIN which was provided with your wireless device in the field. Click **Connect** to establish the connection.

PBC: Select this option if your device supports the Push Button Configuration (PBC). Press the PBC button on your wireless device, and click **Connect** within 120 seconds to establish the connection.

Click **Prev** to return to the next step, or click **Cancel** to cancel the setup wizard.

STEP 2: CONNECT YOUR WIRELESS DEVICE

There are two ways to add wireless device to your wireless network:
 -PIN (Personal Identification Number)
 -PBC (Push Button Configuration)

☒ **PIN :**

please enter the PIN from your wireless device and click the below "Connect" Button within 120 seconds

☐ **PBC**

please press the push button on your wireless device and click the below "Connect" Button within 120 seconds

Prev Next Cancel Connect

WPS Button: You can also add a wireless device using WPS by pressing the WPS button on the back of the router. To add a new wireless device, first press the WPS button on the back of the router (the Power LED will start to flash). Within 120 seconds, press the WPS button on the device you wish to add. The Power LED will continue to flash while the WPS connection process is in progress. The Power LED will turn solid green to indicate the completion of the WPS process.



If you selected **Manual** as your configuration method in the previous step, a summary will appear showing the current wireless network configuration. You should manually enter this information on your wireless client in order to join the wireless network.

SETUP COMPLETE!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Band : 2.4GHz Band

Wireless Network Name (SSID) : dlink

Security Mode : Auto (WPA or WPA2) - Personal

Cipher Type : TKIP and AES

Pre-Shared Key : password

Manual Wireless Network Setup

From the **Wireless Network** page, you can manually configure your wireless network settings. At any time, you can click the **Save settings** button to save the current configuration and return to the main page, or click **Don't Save Settings** to discard any changes and return to the main page.

If you wish to enable WDS in order to extend an existing wireless network, the following options will be available for configuration.

Enable WDS: Wireless Distribution System (WDS) enables you to use an existing wireless network as the WAN source for your router. This option is typically used if you wish to use *Extender Mode* to extend the reach of an existing wireless network. Check the box to enable WDS.

Wireless Network Name: Enter the network name (SSID) of the wireless network which you want to connect to as your source network. You can also click on the **Site Survey** button to bring up a list of wireless networks within range of your router.

Security Mode: Select the security mode used by the source wireless network.

WPA Mode: Select **Auto** to have the router automatically select the WPA mode based on clients connecting to it, or manually force the router to use **WPA Only** or **WPA2 Only**.

Cipher Type: Select the cipher type used by the source wireless network.

Pre-Shared Key: Enter the pre-shared key of the source network.

Extend SSID: The settings for the extended network such as SSID, channel width, and security mode will remain the same as the source network and cannot be adjusted.

WDS SETTINGS	
Enable WDS :	<input checked="" type="checkbox"/>
Wi-Fi Network Name :	dlink_WDS Site Survey
Security Mode :	WPA-Personal ▼
WPA	
<p>Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.</p> <p>To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher).</p>	
WPA Mode :	WPA Only ▼
Cipher Type :	TKIP ▼
PRE-SHARED KEY	
<p>Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.</p>	
Pre-Shared Key :	password
EXTENDED WIRELESS NETWORK SETTINGS	
Extend SSID :	<input checked="" type="radio"/> Remain the same as SSID <div>dlink_WDS (Also called the SSID)</div>
Channel Width :	20 MHz ▼

Extended Wireless Security Mode: The security settings for the extended network will be the same as those for the source network and cannot be changed.

Pre-Shared Key The pre-shared key for the extended network will be the same as the source network and cannot be changed.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes that have been made.

WPA

Use **WPA** or **WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode :

Cipher Type :

Group Key Update Interval : (seconds)

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key :

If you do not wish to enable WDS, you can configure the wireless settings of your router on this page. The following options will be available for configuration.

Wireless Band: The frequency of the wireless band being configured.

Enable Wireless: Check this box to enable the wireless function of your router.

Wireless Network Name: The network name (SSID) of your wireless network. This name will identify your wireless network.

802.11 Mode: Select one of the following:

- 802.11b Only** - Select if you are only using 802.11b clients.
- 802.11g Only** - Select if you are only using 802.11g clients.
- 802.11n Only** - Select if you are only using 802.11n clients.
- 802.11 Mixed (g/b)** - Select if you are using both 802.11b and 802.11g wireless clients.
- 802.11 Mixed (g/n)** - Select if you are using both 802.11g and 802.11n wireless clients.
- 802.11 Mixed(n/g/b)** - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the router to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the router. By default the channel is set to 6. The channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option can not be selected.

Transmission Rate: Select the wireless data transmission rate. It is strongly suggested to select **Best (Auto)** for best performance.

Channel Width: Select the bandwidth of the wireless channel. It is recommended that this option is set to **20/40 MHz (Auto)** for best performance.

Visibility Status: Select **Visible** to have the router broadcast your SSID to clients within the range of your wireless network. This means that wireless

WIRELESS NETWORK SETTINGS	
Wireless Band : 2.4GHz Band	
Enable Wireless : <input checked="" type="checkbox"/>	
Wireless Network Name :	dlink_WDS (Also called the SSID)
802.11 Mode :	Mixed 802.11n, 802.11g and 802.11b
Enable Auto Channel Scan : <input checked="" type="checkbox"/>	
Wireless Channel :	1
Transmission Rate :	Best (automatic) (Mbit/s)
Channel Width :	20 MHz
Visibility Status : <input checked="" type="radio"/> Visible <input type="radio"/> Invisible	

WIRELESS SECURITY MODE	
Security Mode : WPA-Personal	

WPA	
<p>Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.</p> <p>To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher).</p>	
WPA Mode :	Auto(WPA or WPA2)
Cipher Type :	TKIP and AES
Group Key Update Interval :	3600 (seconds)

PRE-SHARED KEY	
<p>Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.</p>	
Pre-Shared Key :	CB0B7A2DAD

clients will be able to see your wireless network name when they perform a site scan. Select **Invisible** to prevent the router from broadcasting your SSID. In this case, wireless clients will need to manually enter the name of your wireless network in order to connect to it.

Wireless Security Mode: Select your preferred mode of wireless security. For more information regarding how to set up wireless security, please refer to "Wireless Security" on page 47.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes that have been made.

WIRELESS NETWORK SETTINGS	
Wireless Band : 2.4GHz Band	
Enable Wireless :	<input checked="" type="checkbox"/>
Wireless Network Name :	dlink_WDS (Also called the SSID)
802.11 Mode :	Mixed 802.11n, 802.11g and 802.11b ▼
Enable Auto Channel Scan :	<input checked="" type="checkbox"/>
Wireless Channel :	1 ▼
Transmission Rate :	Best (automatic) ▼ (Mbit/s)
Channel Width :	20 MHz ▼
Visibility Status :	<input checked="" type="radio"/> Visible <input type="radio"/> Invisible

WIRELESS SECURITY MODE	
Security Mode :	WPA-Personal ▼

WPA	
<p>Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.</p> <p>To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher).</p>	
WPA Mode :	Auto(WPA or WPA2) ▼
Cipher Type :	TKIP and AES ▼
Group Key Update Interval :	3600 (seconds)

PRE-SHARED KEY	
<p>Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.</p>	
Pre-Shared Key :	CB0B7A2DAD

Network Settings

This section will allow you to configure the local network settings of the router. At any time, you can click the **Save settings** button to save the current configuration and return to the main page, or click **Don't Save Settings** to discard any changes and return to the main page.

- Router IP Address:** Enter the IP address of the router. The default IP address is 192.168.0.1. If you change the IP address, once you click **Save Settings**, you will need to enter the new IP address in your browser address bar in order to access the configuration utility.
- Default Subnet Mask:** Enter the subnet mask. The default subnet mask is 255.255.255.0.
- Enable DNS Relay:** Check the box to transfer the DNS server information from your ISP to your computers.

ROUTER SETTINGS

Use this section to configure the internal network settings of your router. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address :

Default Subnet Mask :

Enable DNS Relay :

☐

DHCP Server Settings

The DIR-610N has a built-in Dynamic Host Control Protocol (DHCP) server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically". When clients connect to the network, they will automatically retrieve the TCP/IP settings provided by the router. The DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

Enable DHCP Server: Check this box to enable the DHCP server on your router. Uncheck to disable this function.

DHCP IP Address Range: Enter the starting and ending IP addresses for the DHCP server's IP assignment pool. This range will determine the last octet of the IP addresses in the DHCP pool. The first three octets will be determined by the router IP address you have defined for the router.

Note: If you statically (manually) assign IP addresses to your computers or devices, make sure that the static IP addresses are outside of this range or you may encounter an IP conflict.

DHCP Lease Time: The length of time for the IP address lease. Enter the lease time in minutes.

DHCP Reservations List: A summary of clients which are currently connected to the router and receiving a reserved DHCP IP address will be listed here.

Number of Dynamic DHCP Clients: Details of computers currently receiving a DHCP address from the router will be displayed here.

DHCP SERVER SETTINGS			
Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.			
Enable DHCP Server : <input checked="" type="checkbox"/>			
DHCP IP Address Range : 100 to 199 (addresses within the LAN subnet)			
DHCP Lease Time : 10080 (minutes)			
DHCP RESERVATIONS LIST			
Host Name	IP Address	MAC Address	Expired Time
NUMBER OF DYNAMIC DHCP CLIENTS			
Host Name	IP Address	MAC Address	Expired Time
07869PCWIN7E	192.168.0.100	cc:52:af:49:e6:9c	6 Days 23 Hours 55 Minutes

DHCP Reservation

If you want a computer or device to always have the same IP address assigned, you can create a DHCP reservation. The router will assign the IP address only to that computer or device.

Note: This IP address must be within the DHCP IP Address Range.

Checkbox: Check the box to the left of the rule to enable DHCP reservations.

Computer Name: Enter the name to identify the computer to which you would like to apply the DHCP reservation. If the computer or device is currently connected to the router, you can choose the name from the drop-down menu and click << to copy the name across.

IP Address: Enter the IP address that you wish to reserve for this device.

MAC Address: Enter the MAC address of the computer or device. If you are making a reservation for a computer currently connected to the router, select the computer from the drop-down menu, and click << to automatically populate the fields.

Click **Save Settings** to save the current configuration.

Click **Don't Save Settings** to discard any changes that have been made.

24 - DHCP RESERVATION

Remaining number of rules that can be created: 24

	Computer Name	IP Address	MAC Address	
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼
<input type="checkbox"/>				<< Computer Name ▼

Advanced Virtual Server

The D-Link DIR-610N can be configured as a virtual server so that remote users accessing web or FTP services via a public IP address can be automatically redirected to local servers in the LAN (Local Area Network). The firewall feature filters out unrecognized packets to protect your LAN so all computers networked with the router are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the router redirects the external service request to the appropriate server within the LAN. The DIR-610N is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer. Each virtual service that is created will be listed at the bottom of the screen in the Virtual Servers List. Pre-defined virtual services are already listed in the table. You may use them by enabling them and assigning the server IP to use that particular virtual service.

D-Link

DIR-610N // SETUP ADVANCED TOOLS STATUS SUPPORT

VIRTUAL SERVER

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings Don't Save Settings

24 - VIRTUAL SERVERS LIST

Remaining number of rules that can be created: 24

	Name	IP Address	Port	Traffic Type
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> 0.0.0.0	Public <input type="text"/> 0	Protocol All
<input type="checkbox"/>	<input type="text"/> << Computer Name	<input type="text"/> 0.0.0.0	Private <input type="text"/> 0	Protocol All

Helpful Hints...

- Check the **Application Name** drop down menu for a list of predefined server types. If you select one of the predefined server types, click the arrow button next to the drop down menu to fill out the corresponding field.
- You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the computer at which you would like to open the specified port.

This will allow you to open a single port. If you would like to open a range of ports, refer to “Port Forwarding” on page 30.

Checkbox: Check the box to the left of the rule to activate that particular virtual server rule.

Name: Enter a name to identify the rule, or select an application from the drop-down menu and click << to automatically populate the fields.

IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the “Computer Name” drop-down menu. Select your computer and click << to populate the field.

Private Port/ Public Port: Enter the port that you want to open next to **Private Port** and **Public Port**. The private and public ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.

Protocol: Select **TCP**, **UDP**, or **All** from the drop-down menu.

Click **Save Settings** to save the current configuration, or click **Don’t Save Settings** to discard any changes.

24 - VIRTUAL SERVERS LIST

Remaining number of rules that can be created: 24

			Port	Traffic Type
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	Public <input type="text" value="0"/>	Protocol All ▼
	IP Address <input type="text" value="0.0.0.0"/>	<< Computer Name ▼	Private <input type="text" value="0"/>	
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	Public <input type="text" value="0"/>	Protocol All ▼
	IP Address <input type="text" value="0.0.0.0"/>	<< Computer Name ▼	Private <input type="text" value="0"/>	

Port Forwarding

Some applications such as multi-player games, media streaming services, and P2P connections require ports to be opened in order to direct incoming packets to the correct computer on your network. The Port Forwarding option will allow you to open a single port or a range of ports.

Checkbox: Check the box to the left of the rule to activate that particular port forwarding rule.

Name: Enter a name for the rule or select an application from the drop-down menu and click << to populate the fields.

IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP) then it will be listed in the “Computer Name” drop-down menu. Select your computer and click <<.

Public Port: Enter the port range that you wish to open on the Internet side.

Private Port: Enter the port range that you wish to open on the LAN side.

TCP/UDP: Depending on the application, enter the TCP and/or UDP port or ports that you want to open.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes.

24 -- PORT FORWARDING RULES

Remaining number of rules that can be created: 24

			Ports to Open		
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	Public Port <input type="text"/> ~ <input type="text"/>		Traffic Type All ▼
	IP Address 0.0.0.0	<< Computer Name ▼	Private Port <input type="text"/> ~ <input type="text"/>		
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	Public Port <input type="text"/> ~ <input type="text"/>		Traffic Type All ▼
	IP Address 0.0.0.0	<< Computer Name ▼	Private Port <input type="text"/> ~ <input type="text"/>		
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	Public Port <input type="text"/> ~ <input type="text"/>		Traffic Type All ▼
	IP Address 0.0.0.0	<< Computer Name ▼	Private Port <input type="text"/> ~ <input type="text"/>		

Network Filters

Network Filters uses MAC (Media Access Control) addresses to allow or deny LAN (Local Area Network) computers from accessing your network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the router.

Configure MAC Filtering: Select **Turn MAC Filtering Off, Allow MAC addresses listed below**, or **Deny MAC addresses listed below** from the drop-down menu.

MAC Address: Enter the MAC address you would like to filter. If the computer you wish to filter is connected to the router as a DHCP client, the computer name will be available for selection from the drop-down menu. Select the desired computer and click << to populate the field.

For more information on how to find a computer’s MAC address, please refer to “Networking Basics” on page 67.

Click **Save Settings** to save the current configuration, or click **Don’t Save Settings** to discard any changes.

24 -- MAC FILTERING RULES

Configure MAC Filtering below:
Turn MAC Filtering ON and ALLOW computers listed to access the network ▼

Remaining number of rules that can be created: 24

	MAC Address		DHCP Client List
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼

Website Filter

Website filters are used to allow you to set up a list of allowed or denied web sites that can be used by multiple users through the network. To use this feature select **Allow** or **Deny**, enter the domain or website and click **Add**, and then click **Save Settings**. For website filters to be enabled, you must also select **Apply Web Filter** under the required policies in the Access Control section.

Configure Website Filter Below: Select **Allow** or **Deny** computers access to only these sites.

Checkbox: Check the box to the left of each field to enable filtering of the website/URL.

Website URL: Enter the websites domains that you want to allow or deny access to.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes.

40 -- WEBSITE FILTERING RULES

Configure Website Filter below:

ALLOW computers access to ONLY these sites

Remaining number of rules that can be created: 40

	Website URL
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

Firewall Settings

A firewall protects your network from the outside world. The DIR-610N offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed completely to the Internet for certain types of applications. If you choose to expose a computer, you can enable DMZ (Demilitarized Zone). This option will completely expose the chosen computer to the Internet.

Enable SPI: Check the box to enable SPI (Stateful Packet Inspection, also known as dynamic packet filtering), which helps to prevent malicious attacks by tracking the state of packets on each session. It validates that the traffic passing through the session conforms to the protocol.

Enable DMZ: If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer. Check this box to enable the DMZ function

DMZ IP Address: Enter the IP address of the computer that you wish to expose to the Internet. If the machine is currently connected to the router, you can select the computer name from the drop-down menu and click << to populate the field.

Note: Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes.

FIREWALL SETTINGS

Enable SPI : ☐

DMZ HOST

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

Enable DMZ : ☐

DMZ IP Address :

<<

Computer Name

Save Settings

Don't Save Settings

Advanced Wireless Settings

This section allows you to configure the advanced setting for the wireless network. The wireless band for this network is fixed at 2.4 GHz.

Transmit Power: Set the transmit power of the antennas.

WMM Enable: WMM is QoS (Quality of Service) for your wireless network. This can improve the quality of video and voice applications for your wireless clients.

Short Guard Interval: Check this box to reduce the guard interval time, which can increase throughput. It can, however, increase the error rate. Enable this option only if it suits your current installation.

HT20/40 Coexistence: Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel over-lapping and causing interference, the router will automatically change to 20 MHz.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes.

ADVANCED WIRELESS SETTINGS

Wireless Band : 2.4GHz Band

Transmit Power :

WMM Enable : ☒ (Wireless QoS)

Short Guard Interval : ☒

HT20/40 Coexistence : ☒ Enable ☐ Disable

Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) is a simplified method for securing your wireless network during the “Initial Setup” and “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across different products and manufacturers. The process is as quick and easy as simply pushing a button (the Push-Button Method) or entering the correct 8-digit code (the PIN-Code Method). The most effective security setting, WPA2, is used automatically.

Enable: Enable the Wi-Fi Protected Setup feature.

Wi-Fi Protected Status: Shows the current status of the WPS function.

Lock WPS PIN Setup: Locking the wireless security settings prevents the settings from being changed by the Wi-Fi Protected Setup feature of the router. Devices can still be added to the network using Wi-Fi Protected Setup. However, the settings of the network will not change once this option is checked. Click the **Reset to Unconfigured** button to clear any current WPS settings.

PIN Settings: A PIN is a unique number that can be used to add the router to an existing network or to create a new network. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator (“admin” account) can change or reset the PIN.

PIN: Shows the current value of the router’s PIN.

Reset PIN to Default: Restore the default PIN of the router.

Generate New PIN: Create a random number that is a valid PIN. This becomes the router’s PIN. You can then copy this PIN to the user interface of the registrar. This wizard helps you add wireless devices to the wireless network.

Connect Your Wireless Device: Starts the WPS connection wizard. For further information on how to add devices to your network using this wizard, please refer to “Add Wireless Device with WPS” on page 19.

Click **Save Settings** to save the current configuration, or click **Don’t Save Settings** to discard any changes.

WI-FI PROTECTED SETUP

Enable : ☒

Wi-Fi Protected Status : Enabled / Configured

Lock WPS-PIN Setup : ☐

Reset to Unconfigured

PIN SETTINGS

PIN : 36527151

Reset PIN to Default Generate New PIN

ADD WIRELESS STATION

Connect your Wireless Device

Save Settings Don't Save Settings

Advanced Network Settings

UPnP Settings: To use the Universal Plug and Play (UPnP) feature click **Enable UPnP**. UPnP provides compatibility with networking equipment, software and peripherals.

Enable WAN Ping Response: Unchecking the box will not allow the router to respond to pings. Blocking the ping may provide some extra security from external threats. Check the box to allow the Internet port to be “pinged”.

WAN Port Speed: You may set the port speed of the Internet port to **10 Mbps, 100 Mbps**, or **Auto 10/100 Mbps**. Some older cable or DSL modems may require you to set the port speed to 10 Mbps.

Enable Multicast Streams: Check the box to enable the router to receive multicast streams over IPv4.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes.

UPNP
Universal Plug and Play(UPnP) supports peer-to-peer Plug and Play functionality for network devices.
Enable UPnP : <input checked="" type="checkbox"/>

WAN PING
If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.
Enable WAN Ping Response : <input type="checkbox"/>

WAN PORT SPEED
WAN Port Speed : Auto 10/100Mbps ▼

MULTICAST STREAMS
Enable Multicast Streams : <input type="checkbox"/>

Save Settings

Don't Save Settings

Tools

Administrator Settings

This page will allow you to change the administrator password and configure remote management of your router. You can also enable Remote Management. At any time during the setup process, you can click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes.

Admin Password: Enter a new password for the Administrator account. The administrator can make changes to the settings. Enter the new password in the **Password** field, and again in the **Verify Password** field.

Enable Remote Management: Remote management allows the router to be configured from the Internet by a web browser. A username and password is still required to access the web-management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

Remote IP Address: Enter the IP address which can be used to remotely access the router.

Remote Admin Port: The port number used to access the router.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes.

D-Link

DIR-610N //

SETUP ADVANCED **TOOLS** STATUS SUPPORT

ADMINISTRATOR SETTINGS

The 'admin' account can access the management interface. The admin has read/write access and can change password.
By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

Save Settings Don't Save Settings

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password :
Verify Password :

ADMINISTRATION

Enable Remote Management : ☒
Remote Ip Address :
Remote Admin Port :

Save Settings Don't Save Settings

Helpful Hints...

- For security reasons, it is recommended that you change the password for the Admin account. Be sure to write down the new password to avoid having to reset the router in case they are forgotten.

Time and Date

The Time and Date configuration option allows you to configure, update, and maintain the correct time on the internal system clock. In this section you can set the time zone that you are in and set the time server. Daylight saving can also be configured to automatically adjust the time when needed.

Time: Displays the current system time and date.

Time Zone: Select your current time zone from the drop-down menu.

Daylight Saving: Check the box to enable automatic adjustment for daylight saving time.

Sync. Your Computer's Time Settings: Click to synchronize the router's time and date settings with the local PC.

Automatic Time and Date Configuration: Check the box to automatically synchronize the router's time and date settings with D-Link's Internet time server.

NTP Server Used: Select the preferred Network Time Protocol (NTP) server from the drop-down menu. Once selected, click **Update Now** to synchronize the router's time and date settings with the NTP server.

Set the Time and Date Manually: To manually input the time, enter the values in these fields for the year, month, day, hour, minute, and second.

Click **Save Settings** to save the current configuration, or click **Don't Save Settings** to discard any changes.

TIME AND DATE CONFIGURATION

Time : 2000/01/01,00:10:07
Time Zone : [(GMT+08:00) Taipei]
Enable Daylight Saving : ☐

Sync. your computer's time settings

AUTOMATIC TIME AND DATE CONFIGURATION

☐ Automatically synchronize with D-Link's Internet time server
NTP Server Used : [Select NTP Server]

Update Now

SET THE TIME AND DATE MANUALLY

Year [2013]
Month [May]
Day [24]

Hour [17]
Minute [6]
Second [53]

Save Settings

Don't Save Settings

System

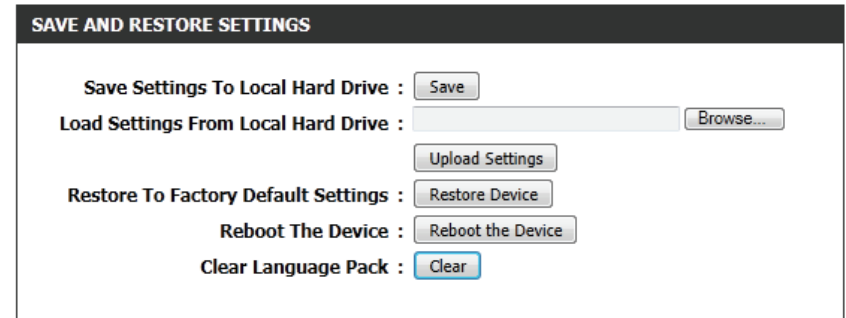
Save Settings to Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** button. You will then see a 'save file' dialog, where you can select a location and file name for the settings.

Load Settings from Local Hard Drive: Use this option to load previously saved router configuration settings. First, click the **Browse** button to locate a saved configuration settings file. Then, click the **Upload Settings** button to transfer those settings to the router.

Restore to Factory Default Settings: Click the **Restore Device** button to restore all configuration settings back to those that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current router configuration settings, use the **Save** button above.

Reboot The Device: Click to reboot the router.

Clear Language Pack: Click the **Clear** button to remove any language packs which have been installed.



The screenshot shows a web interface titled "SAVE AND RESTORE SETTINGS". It contains several sections with buttons:

- Save Settings To Local Hard Drive :** A button labeled "Save".
- Load Settings From Local Hard Drive :** A text input field followed by a "Browse..." button.
- Upload Settings**: A button.
- Restore To Factory Default Settings :** A button labeled "Restore Device".
- Reboot The Device :** A button labeled "Reboot the Device".
- Clear Language Pack :** A button labeled "Clear".

Firmware

You can upgrade the firmware of the router here. Make sure the firmware file you want to use is on the local hard drive of the computer. Please check your local D-Link support site or <http://support.dlink.com> for firmware updates and language packs.

Firmware Information: Displays the current firmware version and date. Click on the **Check Now** button to check for any new firmware updates.

Firmware Upgrade: After you have downloaded the new firmware, click **Browse** to locate the firmware update on your hard drive. Click **Upload** to complete the firmware upgrade.

Language Pack Upgrade: This function allows the user to change the language of the web-based interface from the English default to another language by upgrading the language pack. Click the **Browse** button to locate the desired language pack on your computer. Click **Upload** to load the language pack.

FIRMWARE INFORMATION
Current Firmware Version : 1.00
Current Firmware Date : Mon 22 Apr 2013
Check Online Now for Latest Firmware Version : <input type="button" value="Check Now"/>

FIRMWARE UPGRADE
Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration.
To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.
Upload : <input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Upload"/>

LANGUAGE PACK UPGRADE
Upload : <input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Upload"/>

Dynamic DNS

The DDNS feature allows you to host a server (web, FTP, game server, etc.) using a domain name that you have purchased (www.yourdomain.com) with your dynamically assigned IP address. Most broadband Internet service providers assign dynamic (changing) IP addresses. Using a DDNS service provider, users can enter in your domain name to connect to your server regardless of your IP address.

Enable DDNS: Check the box to enable the DDNS function.

Server Address: Choose your DDNS provider from the drop down menu.

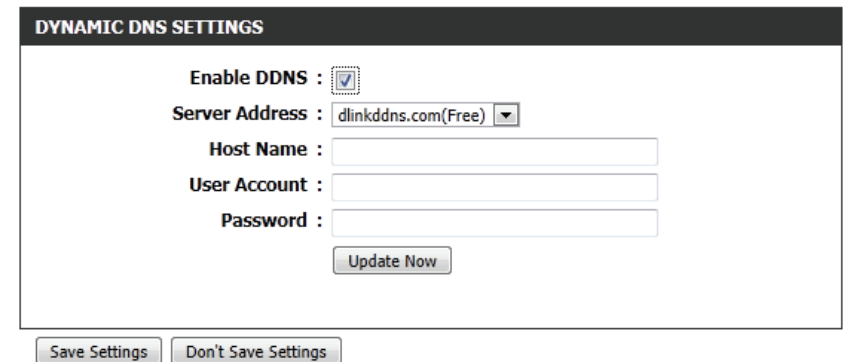
Host Name: Enter the host name that you registered with your DDNS service provider.

User Account: Enter the username for your DDNS account.

Password: Enter the password for your DDNS account.

Click **Update Now** to confirm the settings. The details of the DDNS connection status will be shown below.

Click **Save Settings** to save the current configuration.



The screenshot shows a web interface titled "DYNAMIC DNS SETTINGS". It contains the following fields and controls:

- Enable DDNS :** A checkbox that is checked.
- Server Address :** A dropdown menu with "dlinkddns.com(Free)" selected.
- Host Name :** An empty text input field.
- User Account :** An empty text input field.
- Password :** An empty text input field.
- Update Now** button.
- Save Settings** button.
- Don't Save Settings** button.

Status

Device Information

This page displays the current information for the router. It will display the LAN, WAN (Internet), and Wireless information.

Status information will be shown in the following categories:

General: Displays the router's time and date, as well as the current firmware version and release date.

WAN: Displays the current type of WAN (Internet) connection, and its status. If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP. If your Internet connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection. The connection duration, MAC address, IP address, subnet mask, default gateway, and DNS server addresses will also be displayed here.

LAN: Displays the MAC address, private (local) IP address, and subnet mask for the router. The status of the DHCP server will also be displayed here.

Wireless LAN: Displays the current status of the wireless network. The router's MAC address, current 802.11 mode, channel width, and wireless channel will also be shown. The network name (SSID) will appear in this section, along with details on any wireless security which has been applied to the wireless network.

D-Link

DIR-610N // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO

LOGS

INTERNET SESSIONS

WIRELESS

DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : 2000/01/01,00:10:58

Firmware Version : 1.00 Mon 22 Apr 2013

WAN

Connection Type : DHCP Client

Cable Status : Connected

Network Status : Connected

Renew Release

Connection Up Time : 0 Day 0 Hour 10 Min 31 Sec

MAC Address : 1C:AF:F7:A1:46:51

IP Address : 172.17.5.174

Subnet Mask : 255.255.255.0

Default Gateway : 172.17.5.254

Primary DNS Server : 192.168.168.249

Secondary DNS Server : 192.168.168.201

LAN

MAC Address : 1C:AF:F7:A1:46:50

IP Address : 192.168.0.1

Subnet Mask : 255.255.255.0

DHCP Server : Enabled

WIRELESS

Wireless Radio : Enabled

MAC Address : 1C:AF:F7:A1:46:50

802.11 Mode : 802.11 Mixed(n/g/b)

Channel Width : 20/40MHz

Channel : 10

Network Name (SSID) : dlink

Wi-Fi Protected Setup : Enabled/Configured

Security : WPA/WPA2-PSK

Helpful Hints...

- All of your LAN, Internet and WIRELESS 802.11 N connection details are displayed here.

Logs

The router automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted while logs of the latest events are retained. The **Logs** option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view.

Log Type: Select the type of events that you wish to view from the log:
 System - Displays system events such as web interface logins, DHCP server activity, and WLAN activity.
 Firewall - Shows events related to security such as firewall activity and blocking of potentially malicious activity.
 Security - Shows any changes in the router's status.

Log Level: You can also select the severity level of events which are shown in the log:
 Critical - Events which are critical to the router's operation are shown in the log.
 Warning - Events warning of potential problems are shown in the log.
 Information - General events are shown in the log.

Log Files: Use the buttons in this section to navigate and toggle the log information:
 First Page - Jump to the first page of the log.
 Last Page - Jump to the last page of the log.
 Previous - Jump to the previous page.
 Next - Jump to the next page.
 Clear - Clears all log contents.

LOG TYPE & LEVEL

Log Type: ☒ System ☐ Firewall ☐ Security

Log Level: ☐ Critical ☐ Warning ☒ Information

LOG FILES

First Page Last Page Previous Next Clear

Page 1 / 3

Time	Message
Fri Jan 01 00:00:18 2000	DHCP client: sending DISCOVER ...
Fri Jan 01 00:00:18 2000	DHCP client: sending DISCOVER ...
Fri Jan 01 00:00:19 2000	DHCP client: sending DISCOVER ...
Fri Jan 01 00:00:22 2000	DHCP Server Starting
Fri Jan 01 00:00:24 2000	DHCP client: sending DISCOVER ...
Fri Jan 01 00:00:24 2000	DHCP client: receive OFFER from 172.17.102.210.
Fri Jan 01 00:00:24 2000	DHCP client: sending REQUEST for 172.17.5.174 ...
Fri Jan 01 00:00:26 2000	DHCP client: Lease of 172.17.5.174 obtained, lease time 28800
Fri Jan 01 00:00:27 2000	DHCP server: receive REQUEST from cc:52:af:49:e6:9c.
Fri Jan 01 00:00:27 2000	DHCP server: sending NAK to cc:52:af:49:e6:9c.

Internet Sessions

The Internet Sessions page displays the full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

Refresh: Click to refresh the table.

NAPT Sessions: Shows statistics of TCP and UDP sessions.

NAPT Active Sessions: Shows the details of sessions on machines currently connected to the router.

INTERNET SESSIONS

This page display Source and Destination packets passing through the device.

Refresh

NAPT SESSIONS

TCP Sessions : 26

UDP Sessions : 2

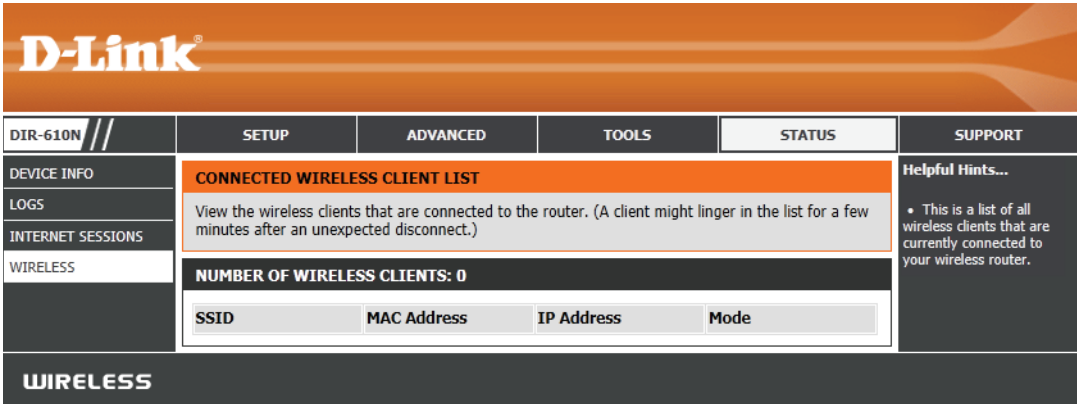
Total : 28

NAPT ACTIVE SESSIONS

IP Address	TCP Sessions	UDP Sessions
192.168.0.100	26	2

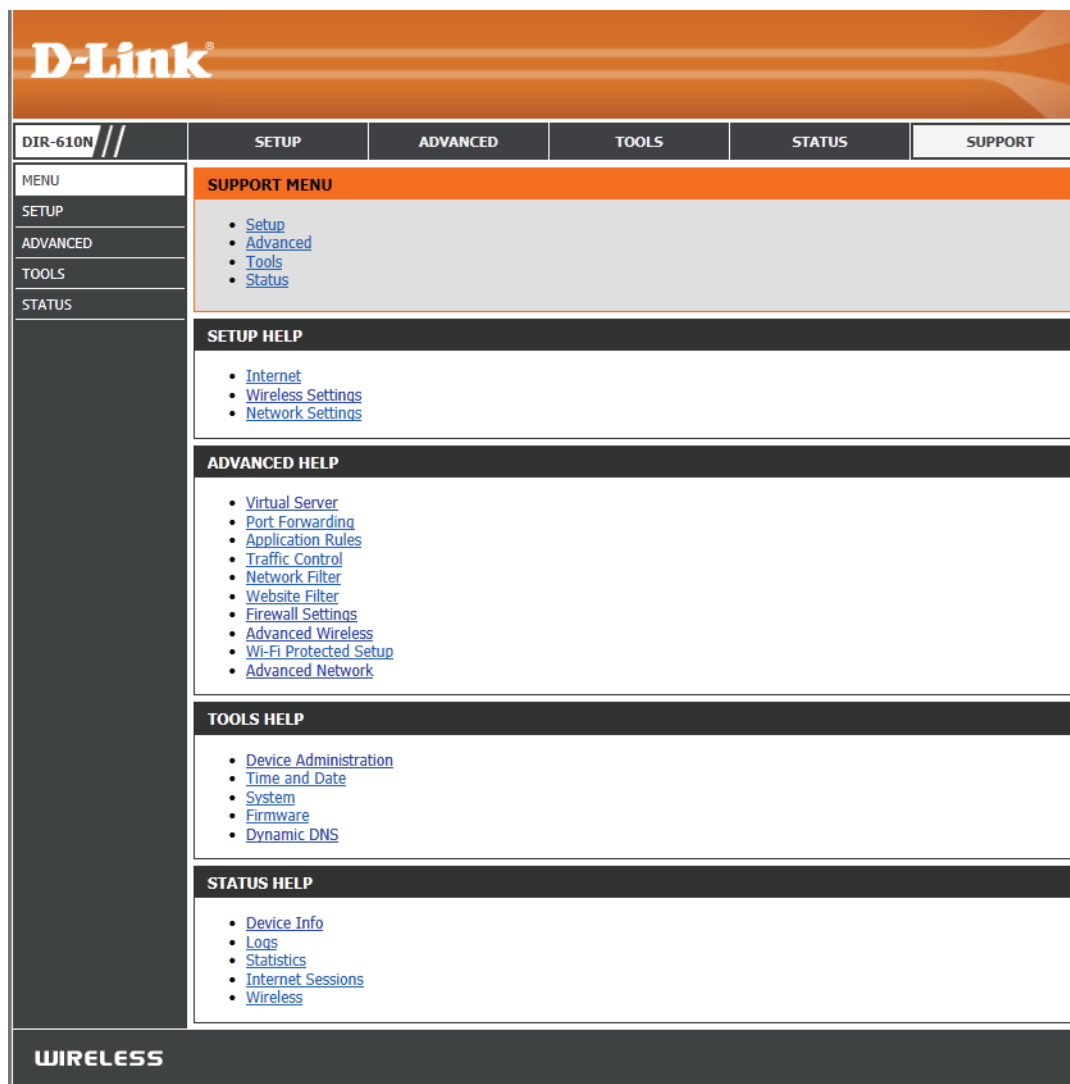
Wireless

The wireless client table displays a list of currently connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.



Support

The Support section provides detailed information on each section of the router's web-based configuration interface. Use the hyperlinks to navigate to the information required.



Wireless Security

This section will show you the different levels of security you can use to protect your network from unauthorized access. The D-Link DIR-610N offers the following types of security:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA/WPA2) - Personal
- Wi-Fi Protected Access (WPA/WPA2) - Enterprise

What is WEP?

Wired Equivalent Privacy (WEP) is an older form of wireless encryption which operates only in 802.11g legacy mode. WEP uses hex digits to create an authentication key, and is considered to be less secure than the newer WPA/WPA2 security standards. It is recommended that you only use this security mode if your wireless clients do not support WPA/WPA2.

What is WPA?

WPA, or Wi-Fi Protected Access, is a Wi-Fi security standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

Configuring WEP

Security Mode: Select **WEP** from the drop-down menu.

WEP Key Length: Select the desired length of the WEP key to be used. In general, a longer key will be more secure than a shorter one. If you select **64 Bit**, the key should consist of 10 hexadecimal digits (0-9 and A-F). You can also enter a key of 5 ASCII characters (0-9, A-Z, and symbols). If you select **128 Bit**, the key should consist of 26 hexadecimal digits, or 13 ASCII characters.

Authentication: Select the desired method of authentication.

WEP Key 1: Enter the desired WEP key (password) according to the WEP key length determined above.

Click **Save Settings** to save the current configuration and return to the home page. Click **Don't Save Settings** to discard any changes and return to the home page.

WIRELESS SECURITY MODE

Security Mode :

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64-bit keys you must enter 10 hex digits into each key box. For 128-bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys, and a maximum of 13 characters for 128-bit keys.

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

WEP Key Length : (length applies to all keys)

Authentication :

WEP Key 1 :

Configuring WPA/WPA2-Personal (PSK)

WPA-Personal is a more modern standard for wireless security on home networks. The WPA standard uses a pre-shared alphanumeric key for authentication. WPA2 is a more recent update to the WPA standard and currently provides the highest level of wireless security for home and personal networks.

Security Mode: Select **WPA-Personal** from the drop-down menu.

WPA Mode: Select the desired WPA mode from the drop-down menu. If you have wireless clients using both WPA and WPA2 encryption, select **Auto (WPA or WPA2)**. If you have only WPA2 clients, select **WPA2 Only**. If you have only WPA clients, select **WPA Only**.

Cipher Type: Select the desired encryption protocol. If you have selected **WPA**, you should select the **TKIP** cipher. If you have selected **WPA2**, you should select the **AES** cipher.

Group Key Update Interval: Enter the period of time between group key update intervals. The default value is 3600 seconds.

Pre-Shared Key: Enter the desired pre-shared key (password) for your wireless network. Wireless clients will need this password in order to access your network. The password should be between 8 and 63 alphanumeric characters in length. It is recommended that you use a combination of numbers and letters in your password for increased security.

Click **Save Settings** to save the current configuration and return to the home page. Click **Don't Save Settings** to discard any changes and return to the home page.

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key :

Save Settings Don't Save Settings

Configuring WPA/WPA2-Enterprise (PSK)

WPA-Enterprise uses the WPA security standard for the security of larger, enterprise-level networks. WPA-Enterprise uses the 802.1x standard to authenticate clients through a remote RADIUS server, therefore providing an increased level of security for large networks. Contact your network administrator if you do not have all of the information required for this configuration.

Security Mode: Select **WPA-Enterprise** from the drop-down menu.

WPA Mode: Select the desired WPA mode from the drop-down menu. If you have wireless clients using both WPA and WPA2 encryption, select **Auto (WPA or WPA2)**. If you have only WPA2 clients, select **WPA2 Only**. If you have only WPA clients, select **WPA Only**.

Cipher Type: Select the desired encryption protocol. If you have selected **WPA**, you should select the **TKIP** cipher. If you have selected **WPA2**, you should select the **AES** cipher.

Group Key Update Interval: Enter the period of time between group key update intervals. The default value is 3600 seconds.

RADIUS Server IP Address: Enter the IP address of the remote RADIUS server.

RADIUS Server Port: Enter the port of the remote RADIUS server.

RADIUS Server Shared Secret: Enter the pre-shared secret (password) for the remote RADIUS server. Wireless clients will need this password in order to access the network.

WIRELESS SECURITY MODE

Security Mode : WPA-Enterprise

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

RADIUS server IP Address :

RADIUS server Port : 1812

RADIUS server Shared Secret :

<< Advanced

Optional backup RADIUS server

Second RADIUS server IP Address :

Second RADIUS server Port : 1812

Second RADIUS server Shared Secret :

Save Settings Don't Save Settings

Advanced: Click **Advanced** to display the optional settings for a backup RADIUS server.

Second RADIUS Server IP Address: Enter the IP address of the backup remote RADIUS server.

Second RADIUS Server Port: Enter the port of the backup remote RADIUS server.

Second RADIUS Server Shared Secret: Enter the pre-shared secret (password) for the backup remote RADIUS server. Wireless clients will need this password in order to access the network.

Click **Save Settings** to save the current configuration and return to the home page. Click **Don't Save Settings** to discard any changes and return to the home page.

EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

RADIUS server IP Address :

RADIUS server Port :

RADIUS server Shared Secret :

[<< Advanced](#)

Optional backup RADIUS server

Second RADIUS server IP :
Address

Second RADIUS server Port :

Second RADIUS server Shared :
Secret

[Save Settings](#) [Don't Save Settings](#)

Connect to a Wireless Network

Windows® 8

WPA/WPA2

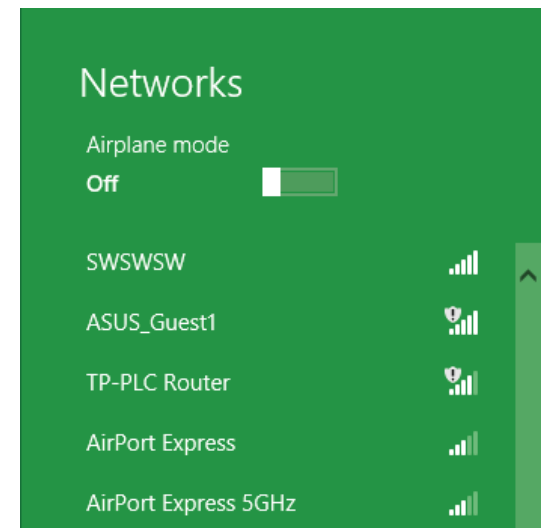
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

To join an existing network, locate the wireless network icon in the taskbar, next to the time display.



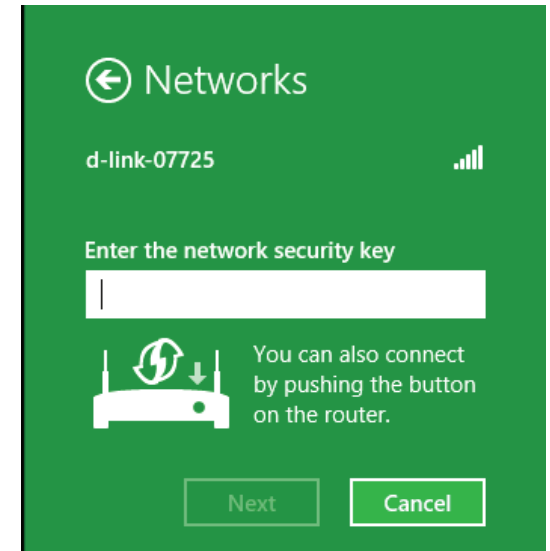
Wireless Icon

Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.

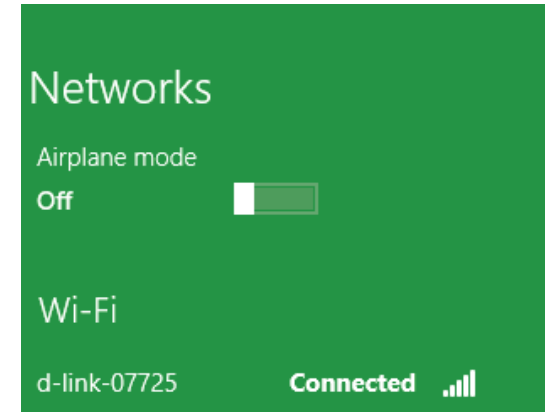


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router at this point to enable the WPS function.



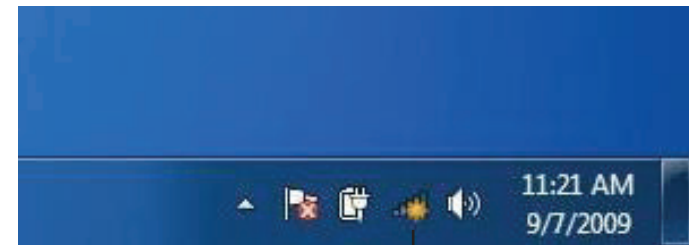
When you have established a successful connection to a wireless network, the word **Connected** will appear next to the name of the network to which you are connected.



Using Windows® 7

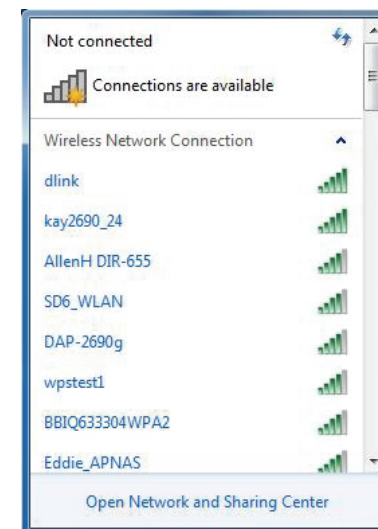
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).



Wireless Icon

2. The utility will display any available wireless networks in your area.

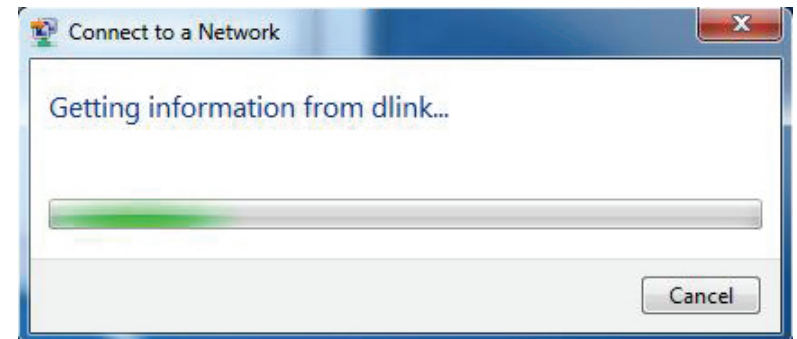


3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

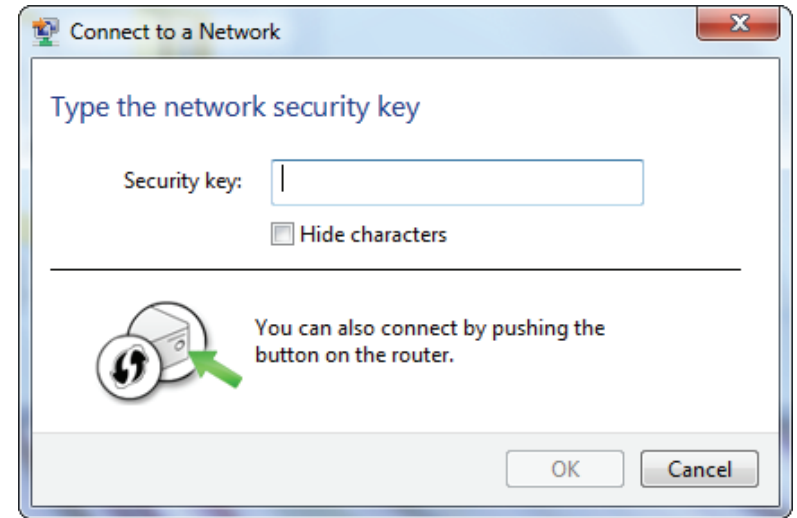


4. The following window appears while your computer tries to connect to the router.



5. Enter the same security key or passphrase that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



Using Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

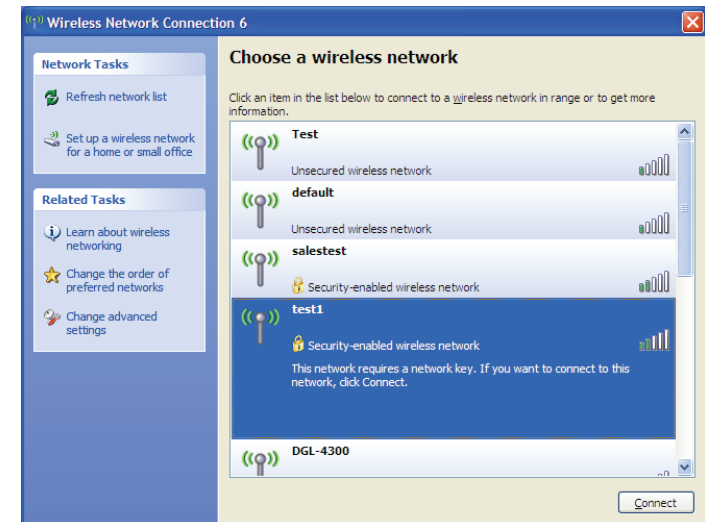
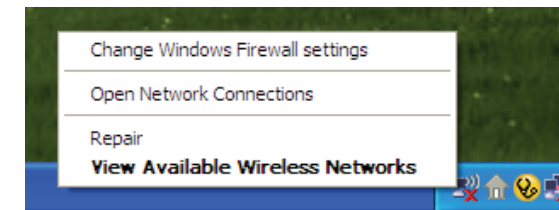
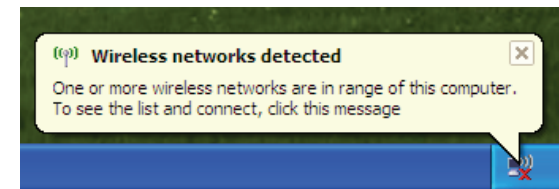
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

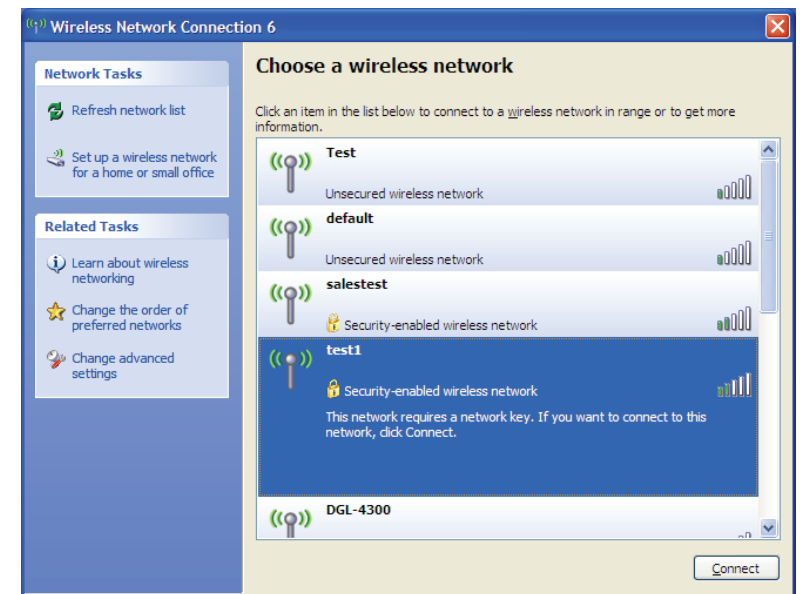
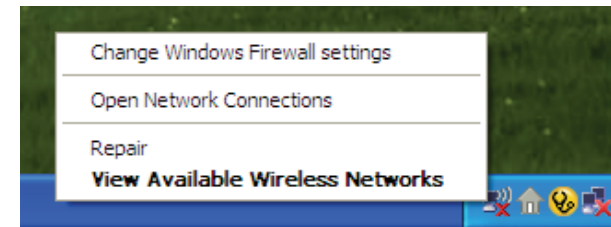
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



Configure WPA-PSK

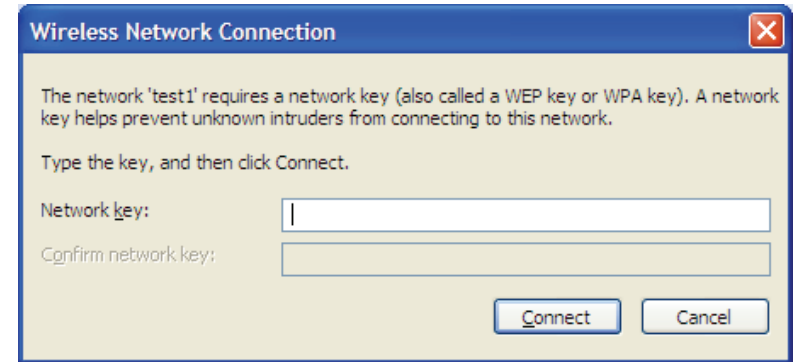
It is recommended to enable WEP on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.
2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK passphrase and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless router.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the D-Link DIR-610N. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screen shots on your computer will look similar to the following examples.)

1. Why can't I access the web-based configuration utility?

When entering the IP address of the D-Link router (192.168.0.1 for example), you are not connecting to a website on the Internet and therefore do not require an Internet connection to do so. The device has the utility built into a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Internet Explorer 8.0 or later
 - Firefox 12.0 or later
 - Safari 4.0 or later (with Java 1.3.1 or higher)
 - Chrome 20.0 or later
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if available. If the computer is turned off, the link light may also be turned off.
- Disable any Internet security software running on the computer. Software firewalls such as ZoneAlarm, BlackICE, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:

- Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** icon. From the **Security** tab, click the button to restore the settings to their defaults.
 - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the **LAN Settings** button. Make sure nothing is checked. Click **OK**.
 - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
 - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your the web management.
 - If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. When logging in, the username is **admin** and leave the password box empty.

3. Why can't I connect to certain sites or send and receive e-mails when connecting through my router?

If you are having a problem sending or receiving e-mail, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (e.g. 1492, 1482, 1472, etc).

Note: AOL DSL+ users must use an MTU of 1400.

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, and XP users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

ping [url] [-f] [-l] [MTU value]

Example: **ping yahoo.com -f -l 1472**

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 203ms, Average = 132ms

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, let's say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network you're working with ($1452+28=1480$).

Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

- Open your browser, enter the IP address of your router (192.168.0.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your e-mail. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapters used on laptop and desktop systems support the same protocols as Ethernet adapters.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A wireless router is a device used to provide this link.

Tips

Here are a few things to keep in mind when you install a wireless network.

Centralize Your Router or Access Point

For best performance, try to place the router/access point in a centralized location within your desired coverage area. Try to place the router/access point as high as possible in the room so the signal gets dispersed throughout your home. If you have a two-story home, you may need an additional access point, or repeater to boost the signal and extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This will significantly reduce any interference that appliances operating on the same frequency might cause.

Security

Don't let unauthorized users connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Please refer to "Wireless Security" on page 47 for further information on how to set up wireless network security.

Wireless Modes

There are two basic modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer for peer-to-peer communication, using wireless network adapters on each computer.

An Infrastructure network contains an access point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

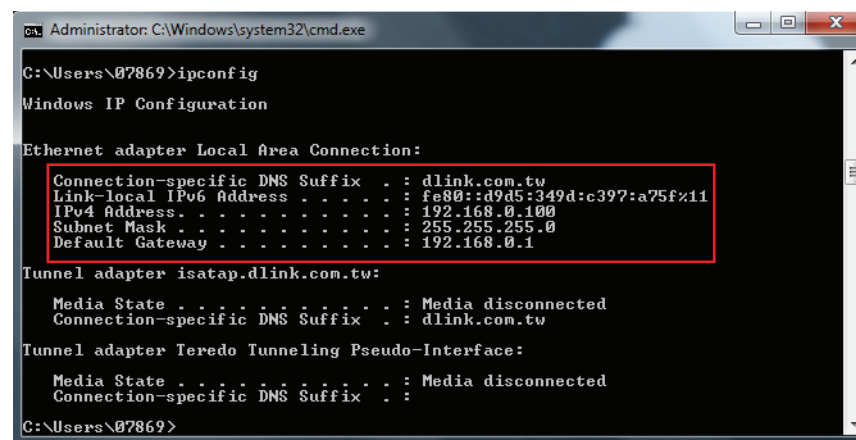
An ad-hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Networking Basics

Check your IP address

After you install your adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

- Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows 8/7/Vista® users can also type **cmd** in the **Start > Search** box.)
- At the prompt, type **ipconfig** and press **Enter**.
- This will display your computer's link-local IPv6 address (if available), IPv4 IP address, subnet mask, and the default gateway of your adapter.
- If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\07869>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : dlink.com.tw
    Link-local IPv6 Address . . . . . : fe80::d9d5:349d:c397:a75f%11
    IPv4 Address. . . . . : 192.168.0.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.dlink.com.tw:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : dlink.com.tw

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\07869>
```

Check Your MAC Address

A Media Access Control (MAC) address is a unique identifier assigned to network adapters to identify them on a network. MAC addresses are also useful for identifying the devices attached to network adapters. If you need to find out your computer's MAC, follow the steps below:

- Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows 8/7/Vista® users can also type **cmd** in the **Start > Search** box.)
- At the prompt, type **ipconfig /all** and press **Enter**.
- Locate your network adapter (you may need to scroll up through the information delivered).
- Your network adapter's MAC address will be displayed as **Physical Address**.

```

WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : dlink.com.tw

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : dlink.com.tw
   Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
   Physical Address. . . . . : CC-52-AF-49-E6-9C
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d9d5:349d:c397:a75f%11(Preferred)
   IPv4 Address. . . . . : 192.168.0.101(Preferred)
   Subnet Mask . . . . . : 255.255.255.0
   Lease Obtained. . . . . : Tuesday, April 16, 2013 8:57:46 AM
   Lease Expires . . . . . : Thursday, April 18, 2013 11:05:57 AM
   Default Gateway . . . . . : 192.168.0.1
   DHCP Server . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . : 248271535
   DHCPv6 Client DUID. . . . . : 00-01-00-01-18-14-5F-3C-CC-52-AF-49-E6-9C

   DNS Servers . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Hamachi:

```


Statically Assign an IP address

If you are not using a DHCP capable gateway/router or you need to assign a static IP address, please follow the steps below:

- Step 1**
- Windows Vista® - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections**.
- Windows® XP - Click on **Start > Control Panel > Network Connections**.
- Windows® 2000 - From the desktop, right-click **My Network Places > Properties**.

Step 2

Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

Step 3

Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4

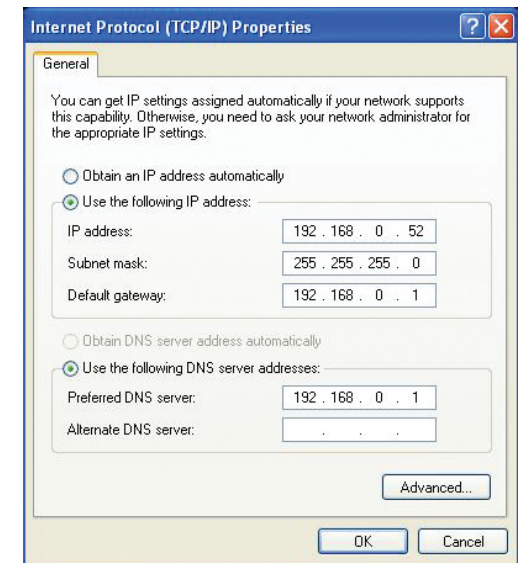
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

Click **OK** twice to save your settings.



Technical Specifications

Interface

- 10/100 Mbps RJ-45 Ethernet LAN Port x 4
- 10/100 Mbps RJ-45 Ethernet WAN Port x 1
- 802.11g/b wireless LAN
- 802.11n compatible wireless LAN

LEDs

- Power
- Internet

Standards

- IEEE 802.11n compatible
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

Security

- WPA/WEP2
 - Personal
 - Enterprise

Wireless Signal Rates*

- 802.11n - Up to 150 Mbps
- 802.11g - Up to 54 Mbps
- 802.11b - Up to 11 Mbps

Operating Frequency

- 2.4 GHz to 2.483 GHz

Antenna Type

- Internal antenna

Temperature

- Operating: 0°C to 40°C (32°F to 104°F)
- Storage: -20°C to 65°C (-4°F to 149°F)

Humidity

- Operating: 10%-90% non-condensing
- Storage: 5%-95% non-condensing

Certification

- FCC, CE
- Wi-Fi Certified

Dimensions

- L = 54 mm (2.12 inches)
- W = 158 mm (6.22 inches)
- H = 113 mm (4.45 inches)

Power Input

- 100-240 V/50-60 Hz
- 5 V DC/0.55 A

Weight

- 164 grams (0.36 lb)

* Maximum wireless signal rate derived from IEEE Standard 802.11g and Draft 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Safety Statements

CE Mark Warning:

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.